UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,094	08/14/2001	Ophir Frieder	IIT-171	8509

7590 05/24/2006

Roland W. Norris
Pauley Petersen Kinne & Fejer
Suite 365
2800 West Higgins Road
Hoffman Estates, IL 60195

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/929,094	FRIEDER ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant's arguments/amendments with respect to originally presented claims 1-27 filed 3/13/2006 have been fully considered but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

In response to Applicants' argument that the present invention is different from the teachings of Lermuzeaux et al. based on the alleged fact that the present invention is "information or data retrieval-based system to detect information content differences in a user's information retrieval patterns and content misuse rather than based upon user action differences as in Lermuzeaux et al." a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. Furthermore, with respects to claims 1 and 14, Examiner would like to point out that the specifics regarding a user's information retrieval patterns and a determination of content misuse are not claimed. Applicants further contends that based on the fact that the cited prior art and the present inventions are allegedly different, that Lermuzeaux provides no suggestion for a security system based on information retrieval patterns. Examiner respectfully disagrees. Lermuzeaux et al. teach various elements that are related to context-clustering thus this reference is highly relevant to the claimed invention (see col. 1, lines 39-47) and provides for the elements of the claimed invention as set forth in the previous office action (pasted below for Applicants' convenience).

Applicants contend that neither of the two references supplies motivation for practicing the limitation of "monitoring families of the digital data gathering results of the user." Examiner respectfully disagrees. Lermuzeaux et al. teach that the digital data that has been gathered is monitored and managed with respect to any flags that are raised which indicate an anomaly (col. 4, lines 9-35). Furthermore, Lermuzeaux et al. teach that monitoring the digital data in this way will help in maintaining a more efficient list of events that are more likely to indicate an anomaly based on the historical facts regarding whether or not a particular event has previously been proven to be anomalous (col. 4, lines 37-42 and col. 4, lines 57-67). Thus, Lermuzeaux et al. teach that the families of digital data gathering results of the user are monitored in order to form better indications of an occurrence of an actual anomaly.

Applicants also contend that neither of the two references supply motivation for practicing the limitations of "comparing the families of the digital data gathering results of the user to the user cluster index to determine anomalies in the digital data gathering results and identifying a potential misuse." Examiner respectfully disagrees. Lermuzeaux et al. teach that when certain rules are broken it shows that the user's behavioral data is not in compliance with the valid rules that were previously established, it indicates anomalous behavior, i.e. potential misuse (col. 3, line 57 – col. 4, line 8). Thus, the user's current behavioral data are compared with the user's valid behavioral data in compliance with the rules established in order to indicate an anomaly and potential misuse when abnormalities are detected. Therefore, Lermuzeaux et al. teach comparing the families of the digital data gathering results of the user to the user cluster index to determine anomalies in the digital data gathering results and identifying a potential misuse.

Applicants further contend that their review of the Lane et al. reference did not find the terms "phrases" and "queries" used in the publication within the context of the present invention. Applicants continue to submit that "none of the cited references teach or suggest the use of information retrieval, including a user lexicon, user cluster index and structured data profile of user characteristics to detect misuse per the limitations of independent claim 15, the ratio of anomalies per claim 16, etc. based on monitoring of information retrieval patterns." Examiner respectfully disagrees. Lermuzeaux et al. teach that the user's previous requests/tasks/objectives which they have accomplished or attempted to carry out are monitored in correspondence to the computer installation requests in order to determine if a current user's request to install a particular application fall within the scope of their role(s) in col. 10, lines 7-31. Thus, Lermuzeaux et al. teach monitoring information retrieval results of a user, as well as maintaining a structured data profile for a user. Furthermore, Lane et al. teach/suggest providing a dictionary created based on the commands/terms most-likely used historically with regards to the user's past queries (page 298 par. 2). Furthermore, the Examiner would like to point out that the teachings of Lane et al. are relevant to the present invention and suggest the scope in which the information presented extends to as seen in the Introduction which shows that this paper "examine[s] the problem of anomaly detection as one of learning to characterize the behaviors of an individual, system, or network in terms of temporal sequences of discrete data. Although here we focus on user-oriented anomaly detection at the level of shell command input, the methods we present are generalizable to learning on arbitrary streams of discrete events such as GUI events, **network packet traffic**, or system call traces" (page 296, lines 1-7). Finally, Oblinger et al. teach/suggest a profile is maintained regarding various domains that a user wishes to search in

context of with respect to the user's historical interactions with the system based on the user's previous "queries, responses, and interactions with the system" (par. 32, lines 10-21). Therefore, Oblinger et al. teach the user cluster index. Since all of these modifications to Lermuzeaux et al. are taught by the prior arts of record, and Lermuzeaux et al. teach a system for detecting misuse, the combination of the cited prior arts of record teach the use of information retrieval, including a user lexicon, user cluster index and structured data profile of user characteristics to detect misuse per the limitations of independent claim 15 based on monitoring of some type of information retrieval patterns. Furthermore, since Lane et al. modifies the combined teachings of the claimed invention in claim 15 to incorporate references to ratios (sec. 2.2.1-2.2.2 on pages 301-302) and thus the combined prior arts of record also teach the ratio of anomalies per claim 16 based on monitoring of some type of information retrieval patterns.

Applicants even further contend that "Parker teaches detecting user habits, such as typing errors, mouse click patterns, etc, namely user interaction; rather than information systems content returned to the user as in the present invention" in reference to claim 8. In response to Applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "rather than information systems content returned to the user") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicants also contend that "none of Parker, Lane, or Lermuzeaux teach or suggest the limitations for practicing the monitoring the digital data gathering results of the user; constructing and maintaining a list of data identifying workplace characteristics of the user and

the use of same to detect a potential misuse." Examiner respectfully disagrees. Lermuzeaux et al. teach that the digital data that has been gathered is monitored and managed with respect to any flags that are raised which indicate an anomaly (col. 4, lines 9-35). Furthermore, Lermuzeaux et al. teach that monitoring the digital data in this way will help in maintaining a more efficient list of events that are more likely to indicate an anomaly based on the historical facts regarding whether or not a particular event has previously been proven to be anomalous (col. 4, lines 37-42 and col. 4, lines 57-67). Thus, Lermuzeaux et al. teach that the families of digital data gathering results of the user are monitored in order to form better indications of an occurrence of an actual anomaly. As for constructing and maintaining a list of data identifying workplace characteristics of the user, Lermuzeaux et al. teach that the user's previous requests/tasks/objectives which they have accomplished or attempted to carry out are monitored in correspondence to the computer installation requests in order to determine if a current user's request to install a particular application fall within the scope of their role(s) in col. 10, lines 7-31. Examiner would like to point out, a user's authorized role is a type of workplace characteristic. Thus, Lermuzeaux et al. teach constructing and maintaining a list of data identifying workplace characteristics of the user and the use of same to detect a potential misuse. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

In this case, Lermuzeaux et al. suggests that maintaining user behaviors over time in order to indicate anomalous behavior when abnormal patterns are detected is well known and very useful in the art (col. 1, lines 39-47).

Applicants further contend that "none of Oblinger, Herz, and Lane teach a system of monitoring an information retrieval system, in the present claims a document collection, for the purposes of maintaining a lexicon and predicting misuse, according to the present invention as a whole." Examiner respectfully disagrees. Lane et al. teach/suggest providing a dictionary created based on the commands/terms most-likely used historically with regards to the user's past queries (page 298 par. 2). Furthermore, the Examiner would like to point out that the teachings of Lane et al. are relevant to the present invention and suggest the scope in which the information presented extends to as seen in the Introduction which shows that this paper "examine[s] the problem of anomaly detection as one of learning to characterize the behaviors of an individual, system, or network in terms of temporal sequences of discrete data. Although here we focus on user-oriented anomaly detection at the level of shell command input, the methods we present are generalizable to learning on arbitrary streams of discrete events such as GUI events, **network packet traffic**, or system call traces" (page 296, lines 1-7). In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Lane

et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated history of the user's behavior are a strong indication of normal usage (sec. 2.2 pages 300-301). Furthermore, in response to applicant's arguments, the recitation "information retrieval system having a document collection" with regards to claims 26-27 has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Finally, Applicants contend that "the Zhang patent has nothing to do with, and provides no suggestion for, a security system based on information retrieval; and therefore provides no motivation to combine with Lane to suggest the elements of the present invention when viewed as a whole." Examiner respectfully disagrees. The teachings/suggestions of Zhang et al. are related to the structural components of the data clustering system. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Zhang et al. suggests

that clustering is highly important so that large amounts of data can be monitored more efficiently (col. 1, lines 18-52).

Due to the reasons stated above, the Examiner maintains rejections with respect to originally presented claims 1-27. The cited prior arts of record in combination with one another teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that originally presented claims 1-27 are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-2, 7, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lermuzeaux et al., US Patent No. 5,621,889 and further in view of Oblinger, US Pub No. 2002/0107852.

As per claim 1:

Lermuzeaux et al. substantially teach a method comprising: a) constructing a user cluster index for a user of a digital data gathering system (col. 7, lines 9-25); b) monitoring families of the digital data gathering results of the user (col. 4, lines 9-67); c) comparing the families of the digital data gathering results of the user to the user cluster index to determine anomalies in the

digital data gathering results (col. 3, line 41 – col. 4, line 2); and d) identifying a potential misuse when an anomaly is detected (col. 3, lines 30-41).

Not explicitly disclosed is wherein the user cluster index comprises a list of families of data to which data from digital data gathering results of the user were categorized. However, Oblinger teaches a system of clustering data based on certain domains that the user wishes to search in context of. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. to construct a user cluster index where the cluster index comprises a list of families of data that are gathered together based on the user's history. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Oblinger suggests the use of an information retrieval system that is organized in such a way that allows a more precise search based on the context chosen and thus has great benefits as shown in paragraphs 32 and 79 of Oblinger.

As per claim 2:

Lermuzeaux et al. and Oblinger substantially teach the method according to claim 1. Furthermore, Lermuzeaux et al. teach the method further comprising: a) comparing the anomalies to the user cluster index to determine the ratio of anomalies to existing clusters; and b) reporting a potential misuse when the ratio exceeds a predetermined threshold (col. 4, lines 36-43).

As per claim 7:

Lermuzeaux et al. and Oblinger substantially teach the method according to claim 1. Furthermore, Lermuzeaux et al. teach the method further comprising: a) constructing a structured

data profile for a user of a digital data gathering system (col. 8, lines 3-15); b) wherein the structured data profile comprises a list of data identifying workplace characteristics of the user (col. 8, lines 3-50); c) comparing the digital data gathering results of the user to the structured data profile to determine whether the digital data gathering results are congruent with the structured data profile (col. 8, lines 3-50); and d) identifying a potential misuse when the digital data gathering results are not congruent with the structured data profile (col. 8, lines 3-50).

As per claim 14:

Lermuzeaux et al. substantially teach a method comprising: a) constructing a structured data profile for a user of a digital data gathering system (col. 7, lines 19-25); c) monitoring digital data gathering results of the user (col. 8, lines 43-50); d) comparing digital data gathering results of the user to the structured data profile to determine whether the digital data gathering results are congruent with the structured data profile (col. 8, lines 43-50); and e) identifying a potential misuse when the digital data gathering results are not congruent with the structured data profile (col. 10, lines 32-40).

Not explicitly disclosed is b) wherein the structured data profile comprises a list of data identifying workplace characteristics of the user. However, Oblinger teaches a system of clustering data based on certain domains that the user wishes to search in context of. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. for the structured data profile to comprise a list of data identifying workplace characteristics of the user. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Oblinger suggests the use of an information retrieval system that is

organized in such a way that allows a more precise search based on the context chosen and thus has great benefits in paragraphs 32 and 79.

III. Claims 3-6 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lermuzeaux et al., US Patent No. 5,621,889 and Oblinger, US Pub No. 2002/0107852 further in view of Lane et al., *Temporal Sequence Learning and Data Reduction for Anomaly Detection.* As per claim 3:

Lermuzeaux et al. and Oblinger substantially teach the method according to claim 1. Furthermore, Lermuzeaux et al. teach the method further comprising: a) monitoring digital data gathering results of the user (col. 4, lines 9-67). Not explicitly disclosed is wherein b) constructing a user lexicon for a user of a digital data gathering system wherein the user lexicon comprises a list of words or phrases gathered from documents of the digital data gathering results of the user. However, Lane et al. teach that based on the user's past queries, a dictionary is created with the most-likely commands/terms used historically by that user. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. for the profile to include a user lexicon of user terms. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated history of the user's behavior are a strong indication of normal usage in section 2.2 (found on pages 300-301).

Also not explicitly disclosed is c) comparing words or phrases gathered from the documents of the digital data gathering results to the user lexicon to determine anomalies in the

digital data gathering results; and d) identifying a potential misuse when an anomaly is detected. However, Lane et al. teach that based on the user's past queries, a dictionary is created with the most-likely commands/terms used and that an anomaly can be detected when the user behavior is determined to be anything other than normal. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. to compare the results of the user to the user profile to determine anomalies from the new queries/results and to identify a potential misuse when detecting an anomaly. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated history of the user's behavior are a strong indication of normal usage in section 2.2 (found on pages 300-301).

As per claim 4:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 3. Furthermore, Lane et al. teach the method further comprising: a) monitoring digital data gathering queries of the user; b) and wherein the user lexicon further comprises a list of words or phrases gathered from the monitoring of the queries; c) comparing queries of the user to the user lexicon to determine anomalies in the queries and d) identifying a potential misuse when an anomaly is detected (sec. 2.2, pages 300-301).

As per claim 5:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 3. Furthermore, Lane et al. teach the method further comprising: a) determining a ratio of

anomalies to words or phrases in the lexicon; and b) reporting a potential misuse when the ratio exceeds a predetermined threshold (sec. 2.2.1-2.2.2 on pages 301-302).

As per claim 6:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 3. Furthermore, Lane et al. teach wherein the user lexicon comprises a list of words or word strings identifying particular words or types of words, or both, extracted from documents returned in response to user queries (sec. 2.2, pages 300-301).

As per claim 9:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 3. Furthermore, Lermuzeaux et al. teach the method further comprising: a) constructing a structured data profile for a user of a digital data gathering system (col. 8, lines 3-15); b) wherein the structured data profile comprises a list of data identifying workplace characteristics of the user (col. 8, lines 3-50); c) comparing the digital data gathering results of the user to the structured data profile to determine whether the digital data gathering results are congruent with the structured data profile (col. 8, lines 3-50); and d) identifying a potential misuse when the digital data gathering results are not congruent with the structured data profile (col. 8, lines 3-50).

IV. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lermuzeaux et al., US Patent No. 5,621,889 and Oblinger, US Pub No. 2002/0107852 and further in view of Parker et al., US Patent No. 5,909,589.

As per claim 8:

Lermuzeaux et al. and Oblinger substantially teach the method according to claim 7. Not explicitly disclosed is the method further comprising: a) the structured data profile comprising a structured data profile lexicon of terms and phrases indicating valid user activity; and b) identifying a potential misuse when the digital data gathering results are not congruent with the structured data profile. However, Parker et al. teach that several questions and responses that would be easily known to the student are stored in order to validate the user and creating an alarm when the words entered by the user are not identical to those stored by the valid user.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. to include a structured data profile with a lexicon of terms/phrases which can indicate valid user activity and to identify a potential misuse when the expected results are not received. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Parker et al. suggest registering student information to be able to differentiate between valid and invalid users in col. 9, lines 17-30 and col. 11, lines 16-55.

V. Claims 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parker et al., US Patent No. 5,909,589 and further in view of Lane et al., *Temporal Sequence Learning and Data Reduction for Anomaly Detection.*

As per claim 10:

Parker et al. substantially teach a method comprising: a) monitoring digital data gathering results of the user (col. 11, lines 16-44); b) constructing a user lexicon for a user of a digital data gathering system (col. 9, lines 22-30); c) comparing words or phrases gathered from the documents of the digital data gathering results to the user lexicon to determine anomalies in the

digital data gathering results (col. 11, lines 16-44); and d) identifying a potential misuse when an anomaly is detected (col. 11, lines 45-55).

Not explicitly disclosed is wherein the user lexicon comprises a list of words or phrases gathered from documents of the digital data gathering results of the user. However, Lane et al. teach that based on the user's past queries, a dictionary is created with the most-likely commands/terms used historically by that user. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Parker et al. for the profile to include a user lexicon of user terms. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated history of the user's behavior are a strong indication of normal usage on page 298, par. 2.

As per claim 11:

Parker et al. and Lane et al. substantially teach the method according to claim 10. Furthermore, Lane et al. teach the method further comprising: a) determining a ratio of anomalies to words or phrases in the lexicon; and b) reporting a potential misuse when the ratio exceeds a predetermined threshold (sec. 2.2.1-2.2.2 on pages 301-302).

As per claim 12:

Parker et al. and Lane et al. substantially teach the method according to claim 10. Furthermore, Lane et al. teach wherein the user lexicon comprises a list of words or word strings identifying nouns extracted from documents returned in response to user queries on page 298, par. 2.

VI. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Parker et al., US Patent No. 5,909,589 and Lane et al., *Temporal Sequence Learning and Data Reduction for Anomaly Detection* and further in view of Lermuzeaux et al., US Patent No. 5,621,889.

As per claim 13:

Parker et al. and Lane et al. substantially teach the method according to claim 10. Not explicitly disclosed is the method further comprising: a) constructing a structured data profile for a user of a digital data gathering system; b) wherein the structured data profile comprises a list of data identifying workplace characteristics of the user; c) comparing the digital data gathering results of the user to the structured data profile to determine whether the digital data gathering results are congruent with the structured data profile; and d) identifying a potential misuse when the digital data gathering results are not congruent with the structured data profile.

However, Lermuzeaux et al. teach the method further comprising: a) constructing a structured data profile for a user of a digital data gathering system (col. 8, lines 3-15); b) wherein the structured data profile comprises a list of data identifying workplace characteristics of the user (col. 8, lines 3-50); c) comparing the digital data gathering results of the user to the structured data profile to determine whether the digital data gathering results are congruent with the structured data profile (col. 8, lines 3-50); and d) identifying a potential misuse when the digital data gathering results are not congruent with the structured data profile (col. 8, lines 3-50).

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. to incorporate attributes such as for workplace characteristics and to use the profile created from a user's history to evaluate normal

usage among users. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lermuzeaux suggests that it's known to monitor user behavior over time in order to detect intrusions in col. 1, lines 39-47.

VII. Claims 15-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lermuzeaux et al., US Patent No. 5,621,889 and further in view of Oblinger, US Pub No. 2002/0107852 Lane et al., *Temporal Sequence Learning and Data Reduction for Anomaly Detection.*

As per claim 15:

Lermuzeaux et al. substantially teach a method comprising: b) the profile including a structured data profile of known user characteristics (col. 7, lines 19-25); c) monitoring information retrieval results of the user (col. 4, lines 9-67); f) comparing the information retrieval results of the user to the structured data profile to determine whether the results are congruent with the structured data profile (col. 8, lines 43-50); and g) identifying a potential misuse when the information retrieval results are not congruent with the structured data profile (col. 10, lines 32-40).

Not explicitly disclosed is a) constructing a profile of use for a user of an information retrieval system. However, Oblinger teaches a system of clustering data based on certain domains that the user wishes to search in context of. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. for the structured data profile to comprise a list of data identifying workplace characteristics of the user. This modification would have been obvious because a person having

ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Oblinger suggests the use of an information retrieval system that is organized in such a way that allows a more precise search based on the context chosen and thus has great benefits in paragraphs 32 and 79.

Also not explicitly disclosed is b) the profile including a user cluster index of result document categories. However, Oblinger teaches a system of clustering data based on certain domains that the user wishes to search in context of. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. to construct a user cluster index where the cluster index comprises a list of families of data that are gathered together based on the user's history. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Oblinger suggests the use of an information retrieval system that is organized in such a way that allows a more precise search based on the context chosen and thus has great benefits in paragraphs 32 and 79.

Also not explicitly disclosed is b) the profile including a user lexicon of user terms. However, Lane et al. teach that based on the user's past queries, a dictionary is created with the most-likely commands/terms used historically by that user. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. for the profile to include a user lexicon of user terms. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated

history of the user's behavior are a strong indication of normal usage in section on page 298, par. 2.

Finally not explicitly disclosed is d) comparing the information retrieval results of the user to the user profile to determine the anomalies in the new queries and results and e) identifying a potential misuse when an anomaly is detected. However, Lane et al. teach that based on the user's past queries, a dictionary is created with the most-likely commands/terms used and that an anomaly can be detected when the user behavior is determined to be anything other than normal. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lermuzeaux et al. to compare the results of the user to the user profile to determine anomalies from the new queries/results and to identify a potential misuse when detecting an anomaly. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated history of the user's behavior are a strong indication of normal usage in section 2.2 (found on pages 300-301).

As per claim 16:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 15. Furthermore, Lane et al. teach the method further comprising: a) determining a ratio of anomalies to words or phrases in the lexicon; and b) reporting a potential misuse when the ratio exceeds a predetermined threshold (sec. 2.2.1-2.2.2 on pages 301-302).

As per claim 17:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 15. Furthermore, Lane et al. teach the method further comprising: weighting potential misuses identified from the user lexicon, the user cluster index, and the structured data profile to determine a report of potential misuse (sec. 2.2.2, page 302, par. 1).

As per claim 18:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 15. Furthermore, Lermuzeaux et al. teach the method further comprising: sending a notification of potential misuse when a potential misuse is identified from two or more of the user lexicon, the user cluster index, and the structured data profile (col. 5, line 61 – col. 6, line 8).

As per claim 19:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 15. Furthermore, Lane et al. teach wherein the user lexicon comprises a list of words or phrases gathered from metadata of documents returned in the query results (sec. 2.2, pages 300-301).

As per claim 20:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 15. Furthermore, Lane et al. teach the user lexicon comprises a list of words, or types of words, or both, extracted from documents returned in the query results (sec. 2.2, pages 300-301).

As per claim 21:

Lermuzeaux et al., Oblinger, and Lane et al. substantially teach the method according to claim 15. Furthermore, Oblinger teaches wherein the user cluster index comprises a list of

families of data to which the data of the user information retrieval results have been categorized (par. 32 and 79).

VIII. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Herz et al., US Patent No. 5,835,087 and further in view of Lane et al., *Temporal Sequence Learning and Data Reduction for Anomaly Detection.*

As per claim 22:

Herz et al. substantially teach a method comprising the steps of: a) pre-clustering the document collection (col. 4, line 35 – col. 5, line 6); b) tracking the cluster from which any document read by the user originates (col. 5, lines 7-20); c) building up a profile of the user based on most frequently accessed clusters over a time sufficient to establish a confidence threshold for validity of the profile of the user (col. 68, lines 63-67); and d) tracking each time the user retrieves and reads a document outside of the most frequently accessed clusters (col. 7, lines 11-45).

Not explicitly disclosed is e) establishing a misuse threshold number for documents read outside of the most frequently accessed clusters and after the misuse threshold number is obtained, signaling that a potential misuse may have occurred. However, Lane et al. teach that based on the user's past queries, a dictionary is created with the most-likely commands/terms used and that an anomaly can be detected when the user behavior is determined to be anything other than normal. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Herz et al. to establish a threshold indicating a misuse has occurred when enough documents that are not in the cluster of the most frequently accessed documents are accessed and to identify a potential misuse when detecting an

anomaly. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior and the accumulated history of the user's behavior are a strong indication of normal usage in section 2.2 (found on pages 300-301).

IX. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lane et al., *Temporal Sequence Learning and Data Reduction for Anomaly Detection* and further in view of Zhang et al., US Patent No. 5,832,182.

As per claim 23:

Lane et al. substantially teach a method comprising the steps of: a) retrieving documents in response to user queries (sec. 2.2.1 on page 301); b) clustering the retrieved documents by category (sec. 2.2.2 on pages 301-303); and d) determining if a sufficient number of retrieved documents do not participate in any valid cluster and if not, sounding an alarm (sec. 2.2.3 – 2.2.4 on pages 303-304).

Not explicitly disclosed is c) establishing and obtaining a threshold number of retrieved documents and after the threshold number of retrieved documents is obtained, determining a size for each clusters, and further denoting clusters of a large enough size as valid clusters. However, Zhang et al. teach keeping track of cluster sizes so that one cluster does not become excessively large. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lane et al. to monitor the number of documents retrieved so that once a threshold number of them are retrieved determining if the size is valid. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Zhang et al. suggest

that the data is clustered in the correct cluster and not clustered where it does not belong in col. 19, lines 5-16 and col. 19, lines 46-52.

X. Claims 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lane et al., *Temporal Sequence Learning and Data Reduction for Anomaly Detection* and further in view of Herz et al., US Patent No. 5,835,087.

As per claim 24:

Lane et al. substantially teach a method comprising the steps of: a) identifying top weighted terms from documents retrieved by the user and storing the top weighted terms in a user-specific lexicon (sec. 2.2.1 on page 301); c) identifying for each new query, if the top weighted terms are in the user-specific lexicon (sec. 2.2.2 on pages 301-303); d) tracking a ratio of newly occurring terms to existing user-specific lexicon terms (sec. 2.2.2 on pages 301-303); and e) if the ratio of newly occurring terms to existing user-specific lexicon terms exceeds a threshold, sending an alarm (sec. 2.2.3 – 2.2.4 on pages 303-304).

Not explicitly disclosed is b) tracking user activity until the rate of new terms added slows and the user-specific lexicon stabilizes to form a user profile. However, Herz et al. teach monitoring users' search queries and an updating the profile in order to maintain a relevant profile. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Lane et al. to track user activity until the rate of new terms added slows and the user-specific lexicon stabilizes to form a user profile. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Herz et al. suggests that it is important to maintain an updated user search profile in order to avoid long exhaustive

searches by implementation of this system in col. 1, lines 45-49 and col. 4, line 35 - col. 5, line 30.

As per claim 25:

Lane et al. and Herz et al. substantially teach the method according to claim 24. Furthermore, Herz et al. teach the method, further comprising the steps of: a) tagging the documents to identify words in the documents by type (col. 12, lines 47-67); b) running an original query of terms and phrases (col. 12, lines 6-46); c) selecting specific types of words from relevant documents retrieved by the original query and adding these terms to a second query (col. 12, line 47 – col. 13, line 23); and d) iteratively selecting specific types of words from relevant documents retrieved by each query and adding the selected specific types of words to a further query to filter the user-specific lexicon (col. 13, line 24 – col. 14, line 2).

XI. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Oblinger, US Pub No. 2002/0107852 and further in view of Lane et al., *Temporal Sequence Learning and Data Reduction for Anomaly Detection.*

As per claim 26:

Oblinger substantially teaches a method, comprising the steps of: a) identifying structured data sources that can be used to identify what the user is working on (par. 49 and par. 60, lines 1-9) and b) querying these sources and, for each source, mapping a structured result into a structured data lexicon of terms and phrases that indicate valid user activity (par. 60, lines 9-20). Not explicitly disclosed is c) for each new query, tracking a ratio of terms found in the structured data lexicon to those not found in the structured data lexicon; and d) if the ratio exceeds a threshold, sending an alarm that a misuse may have occurred.

However, Lane et al. teach that a similarity function is used in order to determine a ratio of terms that occur in the user's dictionary and those that don't thereby determining an anomaly if the similarity value is not high enough. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Oblinger to track a ratio of terms found in the structured data lexicon to those not found in the structured data lexicon and to send an alarm that a misuse may have occurred if a certain threshold is exceeded. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated history of the user's behavior are a strong indication of normal usage in section 2.2 (found on pages 300-301).

XII. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Oblinger, US Pub No. 2002/0107852 and further in view of Herz et al., US Patent No. 5,835,087 and Lane et al., *Temporal Sequence Learning and Data Reduction for Anomaly Detection.*

As per claim 27:

Oblinger et al. substantially teach a method, comprising the steps of: a) identifying structured data sources that can be used to identify what the user is working on (par. 49 and par. 60, lines 1-9); and b) querying the identified structured data sources and, for each source queried, mapping a structured result into a structured data lexicon of terms and phrases that indicate valid user activity (par. 60, lines 9-20).

Not explicitly disclosed is c) for each new query, retrieving relevant documents for that new query and d) extracting key terms from the relevant documents. However, Herz et al. teach

retrieving relevant documents based on the queries entered and updating the user's search history by maintaining the most relevant terms. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Oblinger to retrieve relevant documents for each new query and extracting the key terms from the relevant documents. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Herz et al. suggest that updating the profile is important in order to ensure that the user is retrieving the most relevant data in the most time-efficient manner, in col. 5, lines 7-40 and col. 6, lines 1-18.

Not explicitly disclosed is e) identifying the ratio of key retrieved terms found in the lexicon to those not found in the lexicon; and f) if the ratio exceeds a threshold, sending an alarm that a misuse may have occurred. However, Lane et al. teach that a similarity function is used in order to determine a ratio of terms that occur in the user's dictionary and those that don't thereby determining an anomaly if the similarity value is not high enough. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Oblinger to identify a ratio of terms found in the structured data lexicon to those not found in the structured data lexicon and to send an alarm that a misuse may have occurred if a certain threshold is exceeded. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated history of the user's behavior are a strong indication of normal usage in section 2.2 (found on pages 300-301).

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,370,525
2. US Patent No. 6,594,654
3. US Patent No. 6,446,035
4. US Pub. No. 2002/0042793

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Examiner
Art Unit 2137
5/20/2006

NK

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER